**PCT** WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

| (51) Internationale Patentklassifikation 6 : | | (11) Internationale Veröffentlichungsnummer: |
|---|---|---|
| H04L 9/32 | A1 | WO 98/34373 |
| | | (43) Internationales Veröffentlichungsdatum: 6. August 1998 (06.08.98) |

(21) Internationales Aktenzeichen: PCT/EP98/00303

(22) Internationales Anmeldedatum: 21. Januar 1998 (21.01.98)

(30) Prioritätsdaten:
197 03 929.4 4. Februar 1997 (04.02.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SCHWENK, Jörg [DE/DE]; Südwestring 27, D–64807 Dieburg (DE). HUBER, Klaus [DE/DE]; Rheinstrasse 18, D–64283 Darmstadt (DE).

(81) Bestimmungsstaaten: CA, CN, JP, KR, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
*Mit internationalem Recherchenbericht.*
*Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.*

(54) Title: PROCESS FOR GENERATING A DIGITAL SIGNATURE AND PROCESS FOR CHECKING THE SIGNATURE

(54) Bezeichnung: VERFAHREN ZUM GENERIEREN EINER DIGITALEN SIGNATUR UND VERFAHREN ZUR ÜBERPRÜFUNG DER SIGNATUR

(57) Abstract

A process is disclosed for generating a digital signature s on a message m by means of a secret key comprising at least two large prime numbers p and q. It is provided that s is the zero of the polynomial P(x)–m modulo n, in which P(x) is any permutation polynomial modulo n.

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zum Generieren einer digitalen Signatur s einer Nachricht m mittels eines zumindest zwei große Primzahlen p, q umfassenden geheimen Schlüssels. Es ist vorgesehen, daß s die Nullstelle des Polynoms P(x)–m modulo n ist, wobei P(x) ein beliebiges Permutationspolynom modulo n ist.

*LEDIGLICH ZUR INFORMATION*

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AL | Albanien | ES | Spanien | LS | Lesotho | SI | Slowenien |
| AM | Armenien | FI | Finnland | LT | Litauen | SK | Slowakei |
| AT | Österreich | FR | Frankreich | LU | Luxemburg | SN | Senegal |
| AU | Australien | GA | Gabun | LV | Lettland | SZ | Swasiland |
| AZ | Aserbaidschan | GB | Vereinigtes Königreich | MC | Monaco | TD | Tschad |
| BA | Bosnien-Herzegowina | GE | Georgien | MD | Republik Moldau | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagaskar | TJ | Tadschikistan |
| BE | Belgien | GN | Guinea | MK | Die ehemalige jugoslawische Republik Mazedonien | TM | Turkmenistan |
| BF | Burkina Faso | GR | Griechenland | | | TR | Türkei |
| BG | Bulgarien | HU | Ungarn | ML | Mali | TT | Trinidad und Tobago |
| BJ | Benin | IE | Irland | MN | Mongolei | UA | Ukraine |
| BR | Brasilien | IL | Israel | MR | Mauretanien | UG | Uganda |
| BY | Belarus | IS | Island | MW | Malawi | US | Vereinigte Staaten von Amerika |
| CA | Kanada | IT | Italien | MX | Mexiko | | |
| CF | Zentralafrikanische Republik | JP | Japan | NE | Niger | UZ | Usbekistan |
| CG | Kongo | KE | Kenia | NL | Niederlande | VN | Vietnam |
| CH | Schweiz | KG | Kirgisistan | NO | Norwegen | YU | Jugoslawien |
| CI | Côte d'Ivoire | KP | Demokratische Volksrepublik Korea | NZ | Neuseeland | ZW | Zimbabwe |
| CM | Kamerun | | | PL | Polen | | |
| CN | China | KR | Republik Korea | PT | Portugal | | |
| CU | Kuba | KZ | Kasachstan | RO | Rumänien | | |
| CZ | Tschechische Republik | LC | St. Lucia | RU | Russische Föderation | | |
| DE | Deutschland | LI | Liechtenstein | SD | Sudan | | |
| DK | Dänemark | LK | Sri Lanka | SE | Schweden | | |
| EE | Estland | LR | Liberia | SG | Singapur | | |

# Verfahren zum Generieren einer digitalen Signatur und Verfahren zur Überprüfung der Signatur

Die Erfindung betrifft ein Verfahren zum Generieren einer digitalen Signatur einer Nachricht mittels eines zumindest zwei große Primzahlen umfassenden geheimen Schlüssels, sowie ein Verfahren zur Überprüfung der Signatur.

Diese Verfahren sind als Public-Key-Signaturverfahren aus der Veröffentlichung von Diffie und Hellmann (W. Diffie, M. E. Hellmann, "New directions in cryptography", IEEE Transactions on Information Theory, Vol. IT-22, November 1976, Seiten 644-654) sowie von Rivest, Shamir und Adleman (R. Rivest, A. Shamir und L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 27, Nr. 2, Februar 1978, Seiten 120-126, RSA-Verfahren) bekannt. Sie verwenden zwei Schlüssel, von denen einer zum Signieren einer Nachricht und ein anderer zum Überprüfen dieser Signatur dient. Dabei wird zum Signieren ein geheimer nur dem Absender der Nachricht bekannter Schlüssel eingesetzt, während für die Überprüfung der Signatur ein öffentlicher Schlüssel verwendet wird. Diese Public-Key-Signaturverfahren werden überwiegend bei der Datenkommunikation mittels elektronischer Medien eingesetzt, wobei die

Signatur als Ersatz für eine Unterschrift dient. Mittels des öffentlichen Schlüssels ist es für den Empfänger der Nachricht möglich, die Echtheit der Signatur und damit des ihm übermittelten Dokuments zu überprüfen. Anwendungsbeispiele zu den obengenannten Signaturverfahren sind in A. Beutelspacher, "Kryptologie", Vieweg-Verlag 1994 genauer beschrieben worden.

Aus der Patentschrift DE 195 13 896 A1 ist ein Public-Key-Signaturverfahren bekannt, bei dem ein Polynom verwendet wird dessen Koeffizienten aus der zu signierenden Nachricht und einer Zufallszahl gebildet werden. Aus diesem auf diese Weise gebildeten Polynom werden zwei weitere Polynome abgeleitet, die mindestens eine Nullstelle in einem endlichen Körper aufweisen müssen, da diese zur Bildung der Signatur verwendet werden. Ist dies nicht der Fall, muß das beschriebene Verfahren mit einer anderen Zufallszahl wiederholt werden.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Signaturverfahren zum Signieren einer Nachricht anzugeben, welches diesen Nachteil nicht aufweist, eine vergleichbare Sicherheit und Ausführungsgeschwindigkeit wie die bisherigen Verfahren aufweist und dabei immer die Generierung einer gültigen Signatur ermöglicht.

Diese Aufgabe wird durch ein Verfahren zum Generieren einer digitalen Signatur mit den Merkmalen des Anspruchs 1 und durch ein Verfahren zur Überprüfung dieser Signatur mit den Merkmalen des Anspruchs 8 gelöst.

Signaturverfahren, die Polynome über dem Ring der Zahlen modulo einer aus mindestens zwei großen Primzahlen bestehenden Zahl n verwenden, sind bereits aus der Literatur bekannt. Das RSA-

Verfahren kann als solches Verfahren aufgefaßt werden. Wichtige Beispiele sind weiterhin die Verfahren, die auf sogenannten Dickson-Polynomen basieren. (W. B. Müller, R. Nöbauer, Cryptanalysis of the Dickson-scheme. Proc. Eurocrypt 85, Lecture Notes in Computer Science, Vol. 219, 1986, Seiten 50-61). Die vorliegende Erfindung geht insoweit über die Arbeiten hinaus, als das Verfahren zur Erzeugung einer Signatur wesentlich allgemeiner ist und es gestattet, auch andere Klassen von Polynomen zu verwenden.

Die Aufgabe der Erfindung wird nun dadurch gelöst, daß eine Nullstelle s des Polynoms $P(x) - m \bmod n$ (oder äquivalent dazu, eine Lösung der Gleichung $P(x) = m \bmod n$) berechnet wird. $P(x)$ muß dabei ein Permutationspolynom modulo n sein (vergleiche Lidl und Niederreiter, Finite Fields, Encyclopaedia of Mathematics Vol. 20, Cambridge University Press 1983) und s stellt die digitale Signatur der Nachricht m dar.

Eine gültige Signatur s der Nachricht m ergibt sich dadurch, daß ein Produkt n aus den beiden Primzahlen p, q gebildet wird und die digitale Signatur s über die Gleichung

$$s = b \cdot u \cdot p + a \cdot v \cdot q \bmod n$$

bestimmt wird und ausgehend von der Gleichung

$$1 = u \cdot p + v \cdot q$$

mittels des erweiterten Euklidischen Algorithmus die Werte u, v und die Werte a, b mittels der Gleichung

$$ggT(P(x)-m,\ x^p-x) \bmod p = x-a$$
$$ggT(P(x)-m,\ x^q-x) \bmod q = x-b$$

berechnet werden und P(x) ein beliebiges Permutationspolynom ist.

In einer Weiterbildung der Erfindung ist vorgesehen, daß der geheime Schlüssel durch die Zahl (p-1)(q-1)+1 aus den Primzahlen p und q gebildet wird und daß die digitale Signatur s nach der Gleichung

$$ggT(P(x) - m, x^{((p-1)(q-1)+1)} - x) \bmod n = x - s$$

gebildet wird. Werden für P(x) Permutationspolynome über einem endlichen Körper verwendet, so ist der größte gemeinsame Teiler, also die Signatur, ein Linearfaktor. Es ist gleichermaßen möglich, statt der oben genannten Zahl (p-1)(q-1)+1 deren äquivalente Zahl zu verwenden, die sich folgendermaßen berechnet:

$$\text{constante} \bullet kgV((p-1),(q-1))+1$$

Eine weitere Ausgestaltung des erfindungsgemäßen Verfahrens besteht darin, daß als Permutationspolynome P(x) verallgemeinerte RSA-Polynome der Form $rx^e + s \bmod n$ oder Tschebyscheff-Polynome $T_e(x) \bmod n$ oder Dickson-Polynome oder aber eine Kombination aus diesen Polynomen verwendet wird. Tschebyscheff-Polynome werden zum Beispiel in I. Schur, "Arithmetisches über die Tschebyscheffschen Polynome", Gesammelte Abhandlungen, Band III, S. 422-453, Springer-Verlag Berlin Heidelberg New York, 1973 behandelt.

Erfindungsgemäß kann vorgesehen werden, daß die Art der Hintereinanderausführung der Tschebyscheff-, verallgemeinerten RSA-, und /oder Dickson-Transformation in Form eines Vektors als Teil des öffentlichen Schlüssels gespeichert wird.

Besonders bevorzugt wird eine Implementierung des Verfahrens, bei dem Permutationspolynome der Form

$rx^e + s \bmod n$ und $ggT(e,(p^2-1)(q^2-1)) = 1$ mit Dickson-Polynomen verschachtelt werden.

Eine weitere vorteilhafte Ausprägung der Erfindung besteht darin, Permutationspolynome der Form

$$P(x) = p^{-1}(x) \circ x^e \circ p(x) \bmod n$$

zu verwenden, wobei $p^{-1}(x)$ das inverse Polynom zu $p(x)$ ist, $p^{-1}(x)$ und $p(x)$ Permutationspolynome modulo n sind, $ggT(e,(p-1)q-1))=1$ gilt und das Symbol "o" die Hintereinanderausführung der zugehörigen Funktion symbolisiert, zum Beispiel $A(x) \circ B(x) = A(B(x))$.

Weitere vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den übrigen Unteransprüchen.

Das im Anspruch 1 genannte Public-Key-Signaturverfahren beruht auf dem mathematischen Problem, zwei große Primzahlen zu faktorisieren. Deshalb werden für den geheimen Schlüssel zwei große Primzahlen benutzt und der öffentliche Schlüssel aus dem Produkt dieser beiden Zahlen gebildet.

Für das erfindungsgemäße Verfahren ist wesentlich, daß neben den beiden Primzahlen Permutationspolynome verwendet werden, die über einem Ring $Z_n$ definiert sind. Ein Permutationspolynom über $Z_n$ ist ein Polynom, das als Funktion betrachtet eine Permutation der Menge $\{0,1,\ldots,n-1\}$ induziert. Einen Überblick über die Theorie der Permutationspolynome ist in dem Buch von Lidl und Niederreiter "Finite Fields", Encyclopaedia of Mathematics Vol. 20, Cambridge University Press 1983 zu finden.

Für das Public-Key-Signaturverfahren werden also für den geheimen Schlüssel zwei große Primzahlen p und q verwendet. Der öffentliche Schlüssel besteht

aus einem Permutationspolynom P(x) und dem Produkt n der Primzahlen p und q.

Soll nun eine Nachricht m von einem Absender signiert werden, so wird zunächst mit Hilfe des Euklidischen Algorithmus der größte gemeinsame Teiler der Polynome $p(x) = P(x) - m \bmod p$ und $x^p-x$ über dem endlichen Körper GF(p) gebildet. Da p(x) ein Permutationspolynom ist, ergibt sich der größte gemeinsame Teiler als Linearfaktor und es gilt

$$ggt(p(x), x^p-x) = x-a$$

In gleicher Weise wird der größte gemeinsame Teiler der Polynome $p(x) = P(x) - m \bmod q$ und $x^q-x$ über dem endlichen Körper GF(q) gebildet. Auch hier ist p(x) ein Permutationspolynom, sodaß der größte gemeinsame Teiler ein Linearfaktor ist, der folgendermaßen berechnet wird

$$ggt(p(x), x^q-x) = x-b$$

Über den erweiterten Euklidischen Algorithmus wird die Beziehung $1 = up + vq$ berechnet, sodaß sich mit den ermittelten Werten a und b die Signatur der Nachricht m berechnen läßt mit

$$s = b \cdot u \cdot p + a \cdot v \cdot q$$

Zur Überprüfung der auf diese Weise gebildeten Signatur beim Empfänger der Nachricht m wird der öffentliche Schlüssel verwendet, der das Permutationspolynom P(x) und das Produkt n der Primzahlen p, q umfaßt. Dazu wird das Polynom $P(x)-m \bmod n$ an der Stelle s ausgewertet, so daß falls die Gleichung

$$P(s)-m \bmod n = 0$$

erfüllt ist, die Gültigkeit der Signatur s bestätigt wird.

Nachfolgend wird das erfindungsgemäße Verfahren zur Signatur einer Nachricht und zur Überprüfung dieser Signatur anhand eines Zahlenbeispiels näher erläutert, wobei der Übersichtlichkeit halber die Zahlenwerte sehr klein gewählt wurden. Als geheimer Schlüssel werden die Primzahlen p=1237 und q=5683 gewählt, so daß das Produkt $n = p \bullet q = 7029871$ ergibt. Der öffentliche Schlüssel ist durch das Polynom $P(x) = 2345678x^5 + 3456789 \bmod n$ und das Produkt n gegeben. Es soll die Nachricht m = 1234567 signiert werden. Mit dem Produkt n ergibt sich das Polynom P(x) zu

$$P(x)-m = 2345678x^5 + 2222222$$

Daran anschließend werden die beiden Polynome

$$p(x) = P(x)-m \bmod p = 326x^5 + 570 \text{ und}$$

$$q(x) = P(x)-m \bmod q = 4282x^5 +169$$

gebildet. Danach können die größten gemeinsamen Teiler der Polynome p(x) beziehungsweise q(x) mit den Polynomen $x^p-x$ beziehungsweise $x^q-x$ berechnet werden:

$$x-a = ggT(326x^5+ 570,\ x^{1237}-x) \bmod p = x + 211$$

$$x-b = ggT(4282x^5+ 169,\ x^{5683}-x) \bmod q = x + 864$$

Dadurch ergeben sich die Werte für a = 1026 und b = 4819.

Aus dem erweiterten Euklidischen Algorithmus ergibt sich mit der Beziehung 1 = up + vq die Darstellung

$$-2683 \bullet p + 584 \bullet q = 1$$

wobei u = -2683 und v = 584 ist (vergleiche E. R. Berkkamp, Algebraic Coding Theory, Aegean Park Press, 1984, S. 21-24).

Mit diesen Werten kann nun die Signatur s berechnet werden:

$$s = -2683 \bullet p \bullet b + 584 \bullet q \bullet a \bmod n = 2022284.$$

Ist die zu signierende Nachricht m größer als das Produkt n, so wird die Nachricht in Blöcke aufgespalten die einzeln signiert werden, oder es wird ein sogenannter Hashwert der Nachricht m signiert.

Zur Überprüfung dieser Signatur kann der öffentliche Schlüssel verwendet werden, der aus dem Polynom P(x) und dem Produkt n gebildet wird. Zur Überprüfung der Signatur muß die Gleichung

$$P(s) - m \bmod n = 0$$

erfüllt sein. Mit den Zahlenwerten ergibt sich, daß s eine gültige Signatur der Nachricht m ist.

Selbstverständlich ist es auch möglich, mehr als zwei Primzahlen als geheimen Schlüssel zu verwenden, wobei das erläuterte Verfahren dann analog auszuführen ist.

**Ansprüche**

1. Verfahren zum Generieren einer digitalen Signatur s einer Nachricht m mittels eines zumindest zwei große Primzahlen p, q umfassenden geheimen Schlüssels, **dadurch gekennzeichnet,** daß s die Nullstelle des Polynoms P(x)-m modulo n ist, wobei P(x) ein beliebiges Permutationspolynom modulo n ist.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,**

- daß ein Produkt n aus den Primzahlen p, q gebildet wird,

- daß die Signatur s mit

$$s = b \bullet u \bullet p + a \bullet v \bullet q \bmod n$$

erzeugt wird, wobei ausgehend von der Gleichung

$$1 = u \bullet p + v \bullet q$$

mittels des erweiterten Euklidischen Algorithmus die Werte u, v und die Werte a, b mittels der Gleichung

$$ggT(P(x)-m,\ x^p-x) \bmod p = x-a$$
$$ggT(P(x)-m,\ x^q-x) \bmod q = x-b$$

berechnet werden.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet,** daß der geheime Schlüssel die Zahl (p-1) (q-1) + 1 oder eine äquivalente Zahl ist und die digitale Signatur s nach der Gleichung

$$ggT(P(x)-m,\ x^{((p-1)(q-1)+1)} - x) \bmod n = x - s$$

berechnet wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß als Permutationspolynome Polynome der Form $r \bullet x^e+s \bmod n$ (verallgemeinerte RSA-Polynome) verwendet werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß als Permutationspolynome Tschebyscheff-Polynome $T_e(x) \bmod n$ verwendet werden.

6. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß als Permutationspolynome Dickson-Polynome verwendet werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß als Permutationspolynome beliebige durch Kombinationen der Tschebyscheff-Polynome, der Dickson-Polynome und der Polynome der Form $r \bullet x^e + s$ erhaltene Polynome verwendet werden.

8. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß die Art der Hintereinanderausführung der Tschebyscheff-, verallgemeinerten RSA-, und/oder Dickson-Transformationen in Form eines Vektors als Teil des öffentlichen Schlüssels gespeichert werden.

9. Verfahren zur Überprüfung einer digitalen Signatur, die gemäß einem Verfahren nach einem der Ansprüche 1 bis 8 gebildet ist, **dadurch gekennzeichnet**, daß ein öffentlicher Schlüssel zur Überprüfung der digitalen Signatur s das Produkt n und ein beliebiges Permutationspolynom P(x) mod n aufweist und daß die digitale Signatur s einer Nachricht m dann gültig ist, wenn die Gleichung

$$P(s)-m \bmod n = 0$$

erfüllt ist.

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 98/00303

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | SCHWENK J ET AL: "PUBLIC KEY ENCRYPTION AND SIGNATURE SCHEMES BASED ON POLYNOMIALS OVER N" ADVANCES IN CRYPTOLOGY - EUROCRYPT '96 INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, SARAGOSSA, MAY 12 - 16, 1996, 12 May 1996, MAURER U (ED ), pages 60-71, XP000577413 see page 61, line 6 - line 8 see page 64, last paragraph - page 65, last line<br>---<br>-/-- | 1 |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 3 June 1998 | 18/06/1998 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Holper, G |

1

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | LIDL R ET AL: "Permutation polynomials in RSA-cryptosystems" ADVANCES IN CRYPTOLOGY. PROCEEDINGS OF CRYPTO 83, SANTA BARBARA, CA, USA, 21-24 AUG. 1983, ISBN 0-306-41637-9, 1984, NEW YORK, NY, USA, PLENUM, USA, pages 293-301, XP002066863 | 1 |
| A | see page 293, last paragraph - page 294, line 31<br>see page 295, paragraph 1 | 5,6 |
| A | DE 195 13 896 A (DEUTSCHE TELEKOM AG) 17 October 1996<br>cited in the application<br>see abstract<br>see column 1, line 25 - column 2, line 24 | 1 |

# INTERNATIONAL SEARCH REPORT

[redacted]mation on patent family members

[redacted]nal Application No
PCT/EP 98/00303

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| DE 19513896 A | 17-10-1996 | AU 4575296 A | 24-10-1996 |
| | | CA 2171143 A | 13-10-1996 |
| | | EP 0739108 A | 23-10-1996 |
| | | NZ 286075 A | 24-06-1997 |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 98/00303

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**
IPK 6 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole )
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

| Kategorie° | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| Y | SCHWENK J ET AL: "PUBLIC KEY ENCRYPTION AND SIGNATURE SCHEMES BASED ON POLYNOMIALS OVER N" ADVANCES IN CRYPTOLOGY - EUROCRYPT '96 INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, SARAGOSSA, MAY 12 - 16, 1996, 12.Mai 1996, MAURER U (ED ), Seiten 60-71, XP000577413 siehe Seite 61, Zeile 6 - Zeile 8 siehe Seite 64, letzter Absatz - Seite 65, letzte Zeile | 1 |

---

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

| Datum des Abschlusses der internationalen Recherche | Absendedatum des internationalen Recherchenberichts |
|---|---|
| 3.Juni 1998 | 18/06/1998 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Holper, G |

1

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| Y | LIDL R ET AL: "Permutation polynomials in RSA-cryptosystems" ADVANCES IN CRYPTOLOGY. PROCEEDINGS OF CRYPTO 83, SANTA BARBARA, CA, USA, 21-24 AUG. 1983, ISBN 0-306-41637-9, 1984, NEW YORK, NY, USA, PLENUM, USA, Seiten 293-301, XP002066863 | 1 |
| A | siehe Seite 293, letzter Absatz - Seite 294, Zeile 31<br>siehe Seite 295, Absatz 1 | 5,6 |
| A | DE 195 13 896 A (DEUTSCHE TELEKOM AG) 17.Oktober 1996<br>in der Anmeldung erwähnt<br>siehe Zusammenfassung<br>siehe Spalte 1, Zeile 25 - Spalte 2, Zeile 24 | 1 |

1

# INTERNATIONAL RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 98/00303

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|---|---|---|---|
| DE 19513896 A | 17-10-1996 | AU 4575296 A | 24-10-1996 |
| | | CA 2171143 A | 13-10-1996 |
| | | EP 0739108 A | 23-10-1996 |
| | | NZ 286075 A | 24-06-1997 |